

コースコード：GX-SAIA

税込価格：165,000円 (税抜価格：150,000円)

日数：1日間

ここに注目!!

【攻撃者視点で選ぶ】

- ・講師は実際に企業へ侵入するペネトレーションテストの専門家
- ・「守り方」だけでなく「攻められ方」から逆算して設計を学ぶ

【攻撃→防御→再攻撃で体験し体得する】

- ・多面的な攻撃シナリオで、自分のAIエージェントの穴を体感
- ・対策を実装し、再攻撃して効果を数値で確認

【一次資料に基づく確かな内容】

- ・OWASP / Anthropic / OpenAI / 12 Factor Agentsの公式文書に基づく
- ・講師の私見ではなく業界の総意。職場で自信を持って展開できる

受講対象者

このトレーニングはこのような方におすすめです。

- ・情報システム部門、セキュリティ担当者
- ・社内開発エンジニア
- ・DX/研修担当者
- ・AIを使ったツールの安全性に責任を持つ立場の方
プログラミング初心者も受講可 (パイプコーディングで補助)

前提条件/前提知識

このコースを受講する前に受講者が習得しておく必要がある知識およびスキルは次のとおりです。

本講座にプログラミング経験は必要ございません。

[認定AIセキュリティエンジニア講座](#)程度のAIに関する基礎知識があれば受講可能です。

目的

このコースを修了すると次のことができるようになります。

本講座は、AIエージェントを活用するだけでなく、AIエージェントの構造や攻撃が成立する仕組みを理解し、「AIエージェントを安全に作り、運用できる」人材の育成を目的としています。

アウトライン

- 10:00～10:50 エージェントとは何か
- 11:00～10:50 AIエージェントの脅威マップ
- 12:50～13:00 パイプコーディングで演習に挑む
- 13:00～14:50 【演習】社内規定Q&Aエージェントを完成させる



15:00 ~ 15:50 【演習】5つの攻撃シナリオで脆弱性を体感する
16:00 ~ 16:30 セキュア設計の原則
16:30 ~ 17:20 【演習】防御実装と再攻撃で効果を検証する
17:30 ~ 17:50 運用フェーズのセキュリティ
17:50 ~ 18:00 まとめ・チェックリスト案内・質疑応答